

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平4-252350

(43) 公開日 平成4年(1992)9月8日

(51) Int.Cl. ⁵	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 15/00	3 3 0 D	7323-5L		
12/14	3 2 0 A	8841-5B		
15/16	4 7 0 M	9190-5L		

審査請求 未請求 請求項の数 1 (全 4 頁)

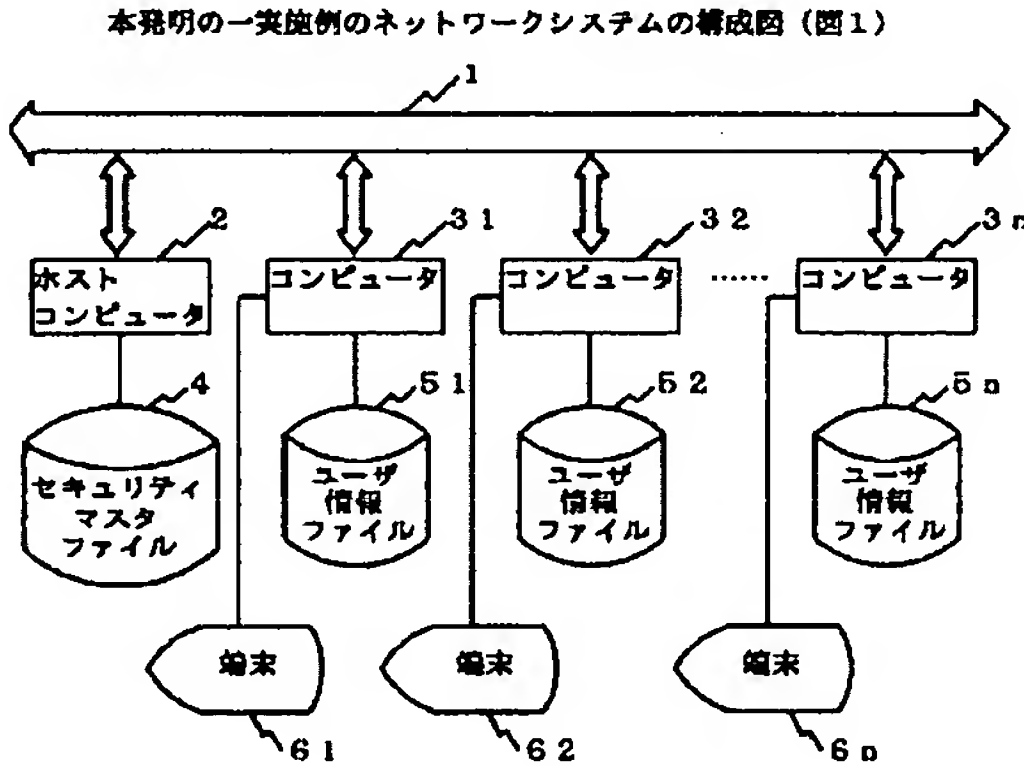
(21) 出願番号	特願平3-8299	(71) 出願人	000005108 株式会社日立製作所 東京都千代田区神田駿河台四丁目6番地
(22) 出願日	平成3年(1991)1月28日	(72) 発明者	小田島 孝 神奈川県横浜市戸塚区戸塚町5030番地 株式会社日立製作所ソフトウェア工場内
		(72) 発明者	織茂 昌之 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内
		(72) 発明者	平澤 茂樹 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内
		(74) 代理人	弁理士 小川 勝男

(54) 【発明の名称】 セキュリティチェック方法

(57) 【要約】

【目的】 不正利用者の積極的な発見のためのセキュリティチェック方法を提供すること。

【構成】 コンピュータ31は、端末61から入力されたユーザID7とパスワード8に、コンピュータ31の持つ端末ID9を附加してセキュリティを強化した上でホストコンピュータ2へ送信する。受信したホストコンピュータ2は、予め登録されたユーザID7とパスワード8と端末ID9と、受信したユーザID7とパスワード8と端末ID9とを比較する。ホスト側コンピュータは、端末61から入力されたユーザID7とパスワード8は一致するが、コンピュータ31が附加した端末ID9が一致しない場合、不正利用者として、予め指定した範囲のアクセスを許可し、使用を継続させ、その間に不正利用者の調査を行う。



1

【特許請求の範囲】

【請求項1】第1のセキュリティ情報を有する第1のコンピュータと、第2のセキュリティ情報を有する第2のコンピュータを有するコンピュータシステムにおいて、該第2のコンピュータは、該第2のコンピュータに入力された第3のセキュリティ情報に該第2のコンピュータが持つ該第2のセキュリティ情報を附加して該第1のコンピュータに送信し、該第1のコンピュータは、受信した該第2、第3のセキュリティ情報と該第1のコンピュータが有する該第1のセキュリティ情報とを比較し、該第3のセキュリティ情報は一致するが、該第2のセキュリティ情報が一致しない場合に、予め指定された範囲のアクセスを許可することを特徴とするセキュリティチェック方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】セキュリティのチェック方法に関する。

【0002】

【従来の技術】従来の方法は、特開平2-208770号公報に記載のように、セキュリティチェックを強化することにより不正な侵入を防止していた。

【0003】

【発明が解決しようとする課題】上記従来技術では、不正な利用者を防止することを目的としており、不正利用者を発見する点での配慮がされておらず、不正利用者が突き止められないという問題があった。

【0004】本発明の目的は、不正利用者の積極的な発見のためのセキュリティチェック方法を提供することにある。

【0005】

【課題を解決するための手段】上記目的を達成するために、第2のコンピュータへ入力される第3のセキュリティ情報に、第2のコンピュータの持つ第2のセキュリティ情報を附加してセキュリティを強化した上で第1のコンピュータへ送信する。第1のコンピュータは、予め登録された第1のセキュリティ情報と受信した第2、第3のセキュリティ情報を比較する。第1のコンピュータは、第2のコンピュータへ入力された第3のセキュリティ情報は一致するが、第2のコンピュータが附加した第2のセキュリティ情報が不一致の場合は、不正利用者の通知を行い、不正利用者として予め指定した範囲でのアクセスを許可し、使用を継続させ、その間に不正利用者の調査を行う。

【0006】

【作用】セッション開始時のチェックは、第2のコンピュータへ入力された第3のセキュリティ情報と第2のコンピュータが附加する第2のセキュリティ情報が、第1のコンピュータに送信され、第1のコンピュータに登録された第1のセキュリティ情報と一致するか否かが確認さ

2

れる。第2のコンピュータへ入力された第3のセキュリティ情報は一致するが、第2のコンピュータが附加した第2のセキュリティ情報が不一致の場合でも、利用者に対しては接続を許可し、使用を継続させて調査する時間をつくと共に、第1のコンピュータは警告を発する。

【0007】

【実施例】以下、本発明の一実施例を図面により詳細に説明する。図1は本発明の一実施例のネットワークシステムの構成図である。ネットワークシステムはネットワーク1により結合されたホストコンピュータ2と複数のコンピュータ31、32、…3nからなる。ホストコンピュータ2はセキュリティマスタファイル4を有する。コンピュータ31、32、…3nはユーザ情報ファイル51、52、…5nと、端末61、62、…6nを有する。

【0008】図2は、セキュリティマスタファイル4とユーザ情報ファイル51、52、…5nのセキュリティ情報10のデータ構成図である。セキュリティ情報10はユーザID7とパスワード8と端末ID9からなる。

【0009】本実施例では、セキュリティ情報10が二重化されている。ホストコンピュータ2のセキュリティマスタファイル4には、予め、ネットワークシステムの全ユーザのユーザID7と、それに対応するパスワード8と端末ID9が登録されている。端末側コンピュータのユーザ情報ファイル51、52、…5nには、各ユーザ毎のユーザID7と、それに対応するパスワード8と端末ID9が登録されている。ユーザ情報ファイル51、52、…5nには、同じユーザID7は登録されない。

【0010】図3は処理の手順を示すフローチャートである。セッション開始時に、利用者がコンピュータ31に接続される端末61から、ユーザID7とパスワード8を入力する（ステップ11）。コンピュータ31内のユーザ情報ファイル51がユーザID7をキーに検索される（ステップ12）。検索できたか否かを判断する（ステップ13）。検索できた場合は、検索の結果得たユーザ情報ファイル51内のパスワード8と、利用者が入力したパスワード8を比較する（ステップ14）。パスワード8が一致したら、ユーザID7とパスワード8と端末ID9からなるセキュリティ情報10をホストコンピュータ2へ送信し、セッション開始要求を行う（ステップ15）。ホストコンピュータ2からの応答を待つ（ステップ16）。検索ができなかった場合、パスワード8が一致しなかった場合は、端末側コンピュータ31はホストコンピュータ2を使用することはできない。

【0011】ホストコンピュータ2はコンピュータ31、32…3nからのセッション開始要求を待つ（ステップ21）。ホストコンピュータ2はセッション開始要求を受信したら、受信したユーザID7をキーにセキュリティマスタファイル4を検索する（ステップ22）。検索

3

できたか否かを判断する(ステップ23)。検索できなかった場合は、セキュリティ情報不正で送信する(ステップ29)。この場合、コンピュータ31は、セッション開始許可情報でないで、セッション開始できない(ステップ17)。

【0012】検索できた場合は、検索の結果得たパスワード8を受信したパスワード8と比較する(ステップ24)。パスワード8が一致しない場合は、セキュリティ情報不正で送信する(ステップ29)。この場合、コンピュータ31は、セッション開始できない(ステップ17)。パスワード8が一致したら、受信した端末ID9と検索の結果得た端末ID9が、一致するかを判断する(ステップ25)。端末ID9が一致したら、正当な利用者として、セッション開始許可情報を送信する(ステップ26)。端末側コンピュータ31は受信した情報がセッション開始許可情報か否かを判断する(ステップ17)。セッション開始許可情報であり、不正利用者ではないので(ステップ18)、コンピュータ31は、正当な利用者として、セッションを開始する。

【0013】ユーザ情報ファイル51に他の端末側コンピュータ用のユーザID7とパスワード8を登録した場合等、パスワード8は一致するが端末ID9が一致しない場合は、まず、ホストコンピュータを管理している者に対して、不正利用者が存在することを通知する(ステップ27)。次に、不正利用者用として予め指定した範囲のアクセス許可をもたせて、セッション開始許可情報を送信する(ステップ28)。端末側コンピュータ31は受信した情報がセッション開始情報か否かを判断する(ステップ17)。セッション開始許可情報であるが、不正利用者なので(ステップ18)、コンピュータ31は、セッションを開始できるが、アクセスできる範囲は、不正利用者用に予め指定された範囲に限られる。このように、不正利用者に使用を継続させて調査する時間をつくり、不正利用者の調査を行う。不正利用者は、正規のユーザID7とパスワード8を入力したので、正規にアクセスできたと思いこむ可能性がある。

【0014】なお、予め指定した範囲のアクセスとは、例えば、見られても実害のないファイルを予めホストコンピュータ2の管理者が指定してその部分のデータを参照させるとか、不正利用者用のダミーのファイルを設定して、そのファイルにのみアクセスを認める等ということである。

【0015】本実施例では、セキュリティ情報10が二重化されており、端末側コンピュータ31、32...3nにおいても、ユーザID7をキーにパスワード8を検索し、一致するか否かをチェックしている。また、端末側コンピュータ31、32...3nが附加する端末ID9は、端末側コンピュータ31、32、...3n毎に対応しておらず、ユーザID7毎に対応している。また、端末ID9は変化しない。

4

【0016】しかし、入力されたユーザID7とパスワード8を端末側コンピュータ31、32...3nでチェックしなくとも良い。また、端末ID9は端末側コンピュータ31、32...3n毎に対応させ、端末側コンピュータ31、32、...3n毎に有する端末ID9を、入力されたユーザID7とパスワード8に附加することにしても良い。また、端末側コンピュータ31、32、...3nが附加する端末ID9を可変にしても良い。

【0017】また、本実施例は、端末側コンピュータ31、32、...3nとホストコンピュータ2から構成されている。しかし、分散型データベースのように、すべてのコンピュータがホストと端末両方の役割を果たすようにしても良い。その場合には、各コンピュータが、自コンピュータにアクセス可能なユーザID7等を登録したファイルを持てば良い。そして、不正利用者がある場合、アクセスされたコンピュータを管理するものに対して、不正利用者の存在することを通知する。

【0018】また、本実施例では、入力されたユーザID7とパスワード8と端末側コンピュータ31、32、...3nが附加した端末ID9が加工されていない。つまり、端末側から送信されたユーザID7とパスワード8と端末ID9と、ホストコンピュータ2が有するユーザID7とパスワード8と端末ID9は同じものである。しかし、ホストコンピュータ2が、予め登録された一定の規則に従って、受信したセキュリティ情報10を加工し、その加工した結果とホストコンピュータ2が有するセキュリティ情報10を比較することにしても良い。また、端末側コンピュータ31、32、...3nが入力されたユーザID7とパスワード8を加工して、送信しても良い。

【0019】本実施例によれば、正規の端末であるコンピュータ32に接続された端末62から他の端末側コンピュータ用のユーザID7とパスワード8を調べてセッションを開始しようとした場合、コンピュータ32にあるユーザ情報ファイル52にユーザID7とパスワード8が登録されていないために、ユーザ情報ファイル52を検索した時点でエラーとなり、ユーザ間でのパスワードの盗用が防止できるという効果がある。

【0020】

【発明の効果】本発明によれば、利用者が入力するセキュリティ情報は一致するが、入力側コンピュータが附加したセキュリティ情報が不一致の場合でも、その不正利用者に対して予め指定された範囲のアクセスを許可し、使用を継続させ、受信側には不正利用者の通知を行い、不正利用者の調査を行うことにより不正利用者の発見が容易であるという効果がある。

【図面の簡単な説明】

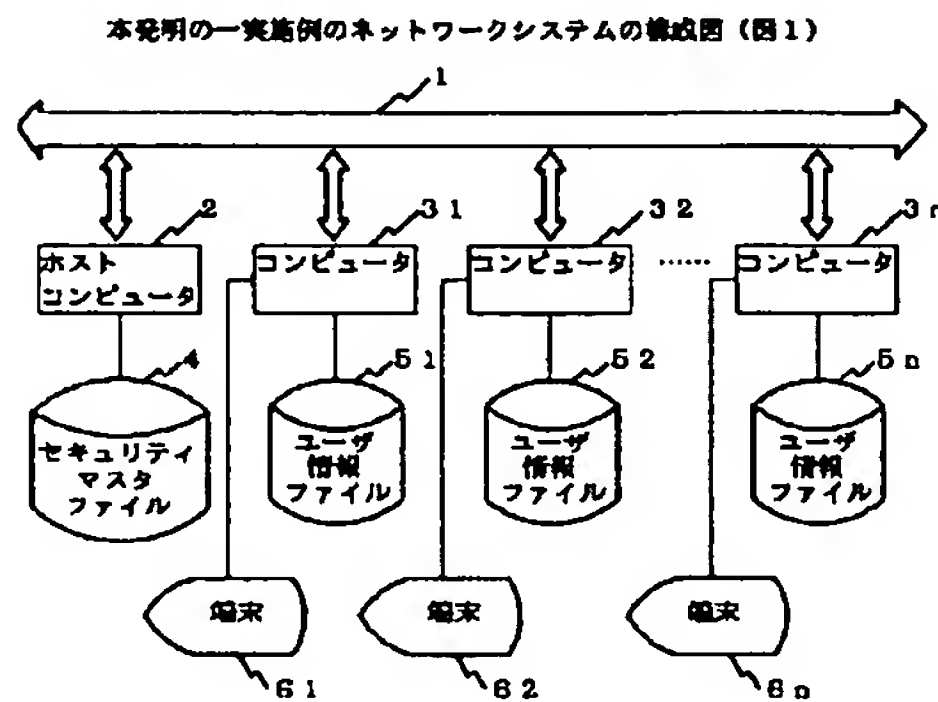
【図1】本発明の一実施例のネットワークシステムの構成図である。

【図2】セキュリティマスタファイルとユーザ情報ファ

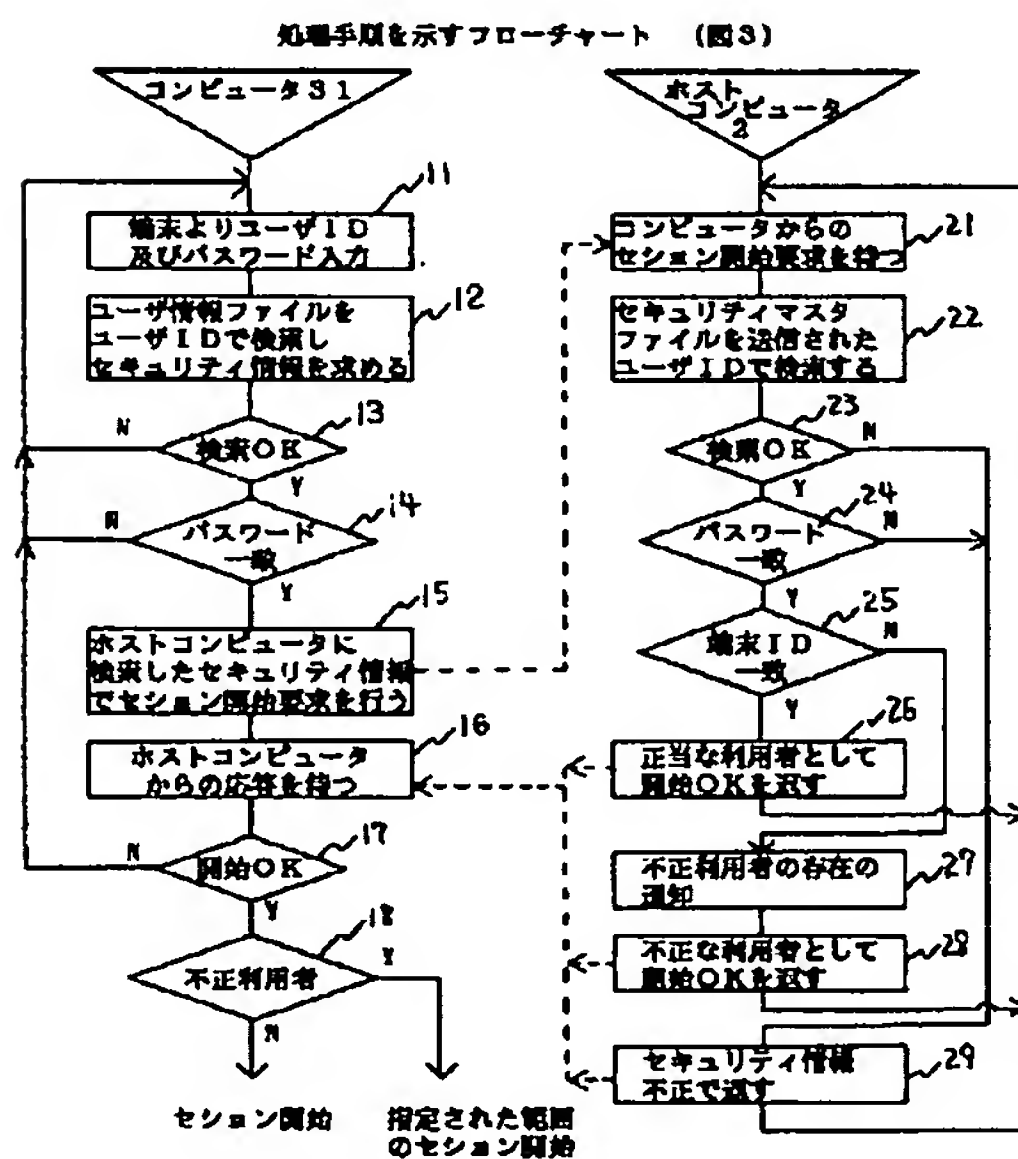
5
 イル内のセキュリティ情報のデータフォーマットを示す図である。
 【図3】 処理手順を示すフローチャートである。
 【符号の説明】
 1…ネットワーク、2…ホストコンピュータ、31, 3

6
 2～3n…コンピュータ、4…セキュリティマスタファイル、51, 52～5n…ユーザ情報ファイル、61, 62～6n…端末、7…ユーザID、8…パスワード、9…端末ID、10…セキュリティ情報。

【図1】



【図3】



【図2】

セキュリティ情報のデータフォーマットを示す図 (図2)

